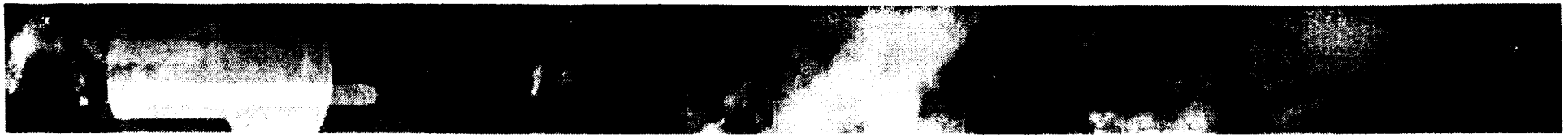
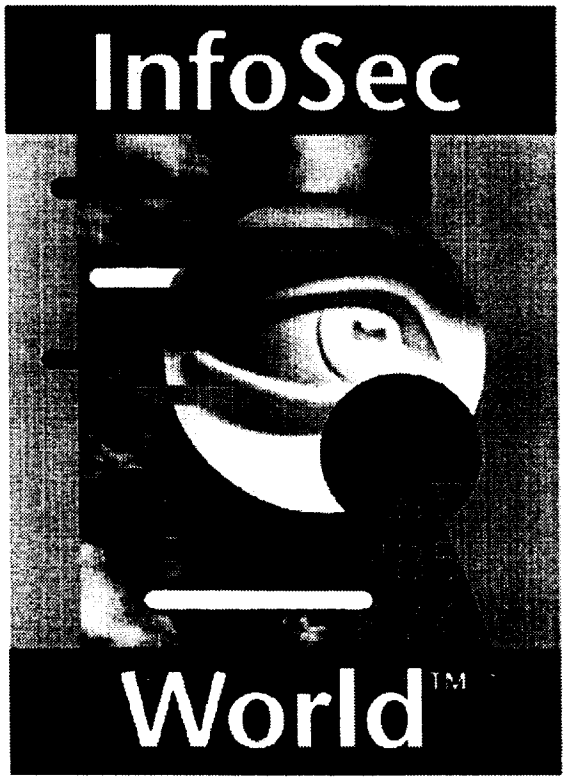




Conference and Expo/2001

MIS TRAINING INSTITUTE

Managing a Vulnerability Testing Program

Session 8

John Ray

Monday, February 26, 2000
10:30AM

InfoSec World Conference Expo/2001

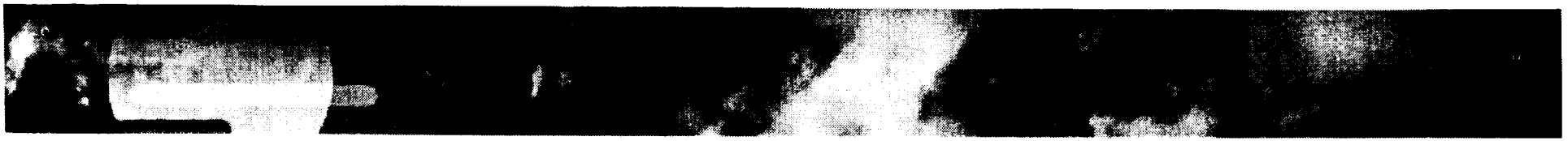
MIS Training Institute

Key Points

- Vulnerability Testing is Essential
- The Approach must be Clear
- Keep the Community Informed
- Set a Target and Report Progress

InfoSec World Conference Expo/2001

MIS TRAINING INSTITUTE



What This Talk is Based On

Security vulnerability testing program, implemented at NASA Ames Research Center from October 1998 to present, which resulted in measurably improved security and a decrease in the number of system compromises experienced.

InfoSec World Conference Expo/2001

Some Background

- Increasing number of system compromises
  - Hackers exploiting known vulnerabilities
  - Excessive down time and costly recovery
  - Bad publicity
- Security program was in place
  - Policies and procedures were in place
  - Roles and Responsibilities were assigned
  - Security bulletins and associated patches were distributed
  - Security training classes were offered
- This alone was no longer sufficient

The Operational Environment

- Campus of over 10,000 networked computers
- Open network
  - Every computer had direct internet access
- Inconsistencies in system administration
  - Uneven application of system security patches
  - Some organizations had no systems administrators
    - Systems "hidden" in research labs
    - Researchers were "systems administrators"

Ideas for a Vulnerability Testing Program

- Use a commercial network security scanner
- Get systems administrators involved
- Identify organizations which need help
- Demonstrate vulnerability
- Provide management with regular reporting
- Demonstrate improvement

Initial Rules and Assumptions

- Select a target set of vulnerabilities - "Top 20"
- Scan the entire campus, organization by organization
- Inform everyone ahead of time when scans will occur
- Do not publish individual vulnerability results
- Make vulnerability scanner software available to all who wanted it
- Perform scans on a regularly scheduled basis

Managing Vulnerability Testing Rolling It Out

- Defining objectives for management
- Preparing for vulnerability testing
- Conducting the test
- Reporting test results
- Achieving compliance
- Lessons learned and pitfalls

InfoSec World Conference Expo/2001

MIS TRAINING INSTITUTE

Defining Objectives for Management

- Explain the problem
- Describe the approach
- Describe the methodology
- Define the Return on Investment (ROI)

InfoSec World Conference Expo/2001

MIS TRAINING INSTITUTE

Explain the Problem

- Describe hacking and exploiting are "known vulnerabilities"
- Use recent events - in your organization or in the News
- Do not forget to include "War Stories" - your or others
- Talk about lost of productivity -
- Talk about liabilities - who has "deep pockets"
- Talk about your company making headline news
- Mention lost of customer confidence -

Describe the Approach

- Define the scope - not a "Big Brother" activity
- Establish the program as a cooperative initiative with System and Network Administrators
- Talk about the training and improving skills aspects
- Explain "Empowerment" and "Buy-in" from sharing the tool
- Talk about the tool and it's capability to provide references needed corrective actions

InfoSec World Conference Expo/2001

MIS Training Institute

Describe the Methodology

- Identify a set target vulnerabilities placing networked systems at risk;
- Establish a metric to track success in reducing the risks from the target vulnerabilities;
- Set a target goal for the metric to meet;
- Conduct scans of all systems for the target vulnerabilities;
- Notify the responsible line mangers and System Administrators of the findings;

Describe the Methodology Cont.

- Set a window for corrective actions to be completed;
- Repeat scans to ensure corrective actions were taken;
- Report vulnerabilities until they are either
  - Signed off as an acceptable risk by a line manager or
  - Corrective actions are taken;
- Evaluate the success of the program in a year;
- Review target vulnerabilities and make adjustments; and
- Set metrics for next goal.

Return on Investment (ROI)

- Estimates cost of resources required
  - Software, hardware, training - one time cost
  - Maintenance for S/W and H/W - on going cost
  - Personnel to conduct testing and analysis results - on going cost
  - Site other organizations' programs for staffing levels and resources

Return on Investment (ROI) Cont.

- Review impacts to the company from a compromised system
  - Lost productivity
  - Lost in customer confidence
  - Liability issues
  - Recover cost - continuity of business
    - Use numbers that will not draw debate (e.g., $50/hr/person)
  - Time spent dealing with news reporters
  - Site real cases and the impact on the victim company

Return on Investment (ROI) Cont.

- Risk of a major compromise vs. cost of a Vulnerability Testing Program
  - Do you have a case?
  - Occurrences per year times cost per occurrence times number of years = risk

    2 x $80,000 x 3 = $480,000
  - One time costs + (maintenance cost + labor cost) times number of years = cost

    60,000 + (8,000 + 80,000) x 3 = $324,000

Points to Remember When Defining Objectives

- Clear and understandable problem
- Open approach with team building, training, and "empowering"
- Well designed result oriented methodology with specific objectives/metrics
- Documented ROI initiative

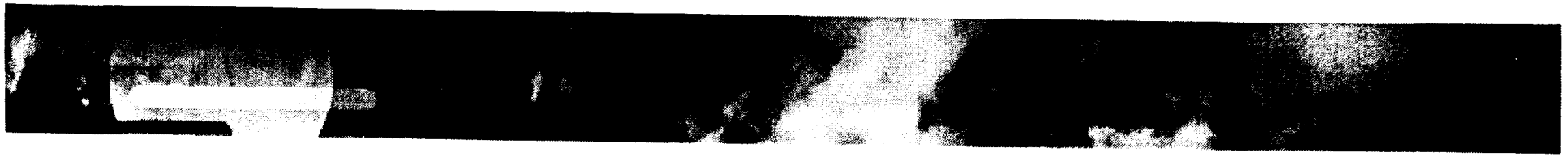
InfoSec World Conference Expo/2001

MIS TRAINING INSTITUTE

Preparing for Vulnerability Testing

- Test Preparation
- Informing the Community
- Scheduling Events

InfoSec World Conference & Expo/2001



Test Preparation

- Identify the systems to be scanned
  - Scan everything - systems, servers, routers, switches, printers, etc.
  - Try to eliminate multiple address for the same system
  - Group the addresses by management organizations
- Identify a target list of vulnerabilities to test
  - Chose exploits which do not give false positives
  - Chose exploits that can be fixed with minimum cost
  - Pick a limited target set to reduce testing time

Test Preparation Cont.

- Train the Staff
  - Ensure those doing the testing get the proper training
  - Train the Help Desk to identify and handle problems arising from scans
- Practice, Practice, Practice
  - Start with a few practice scans
  - How many addresses can you scan at once?
    - Monitor the traffic load on the routers
  - Is the scanner detecting exploits like they should?
  - What do the results look like?

Informing the Community

- Educating the community
  - Raise awareness to the problem
  - Explain the "Vulnerability Testing Program"
  - Ensure the community understands the goals
- Involve the System and Network Administrators
  - Describe the tools being used
  - Offer the tools for self testing
  - Provide training for the tools
  - Establish a Bird-of-Feather (BOF) to share experiences

Informing the Community Cont.

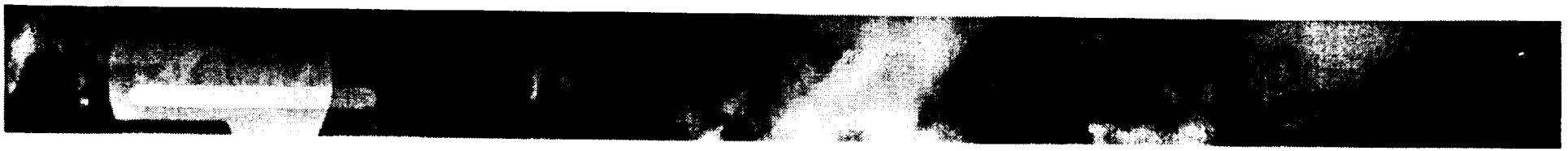
- Met with the line manages that will be receiving the testing results
  - Show them sample reports
  - Demonstrate a vulnerability scan, the results, and the references for taking corrective action
  - Explain the reporting that will be made to senior management

Scheduling Events

- Identify critical systems needing TLC
  - Work closely with the Systems Administrators
  - Schedule off peak testing periods
  - Monitor the testing
- Identify other scheduled activities
  - Central network backups
  - Software management pushes or data pulls
  - Network maintenance and upgrades

Points to Keep in Mind When Preparing for Vulnerability Testing

- Identify what is to be tested
- Learn to use the tools
- Raise the communities awareness
- Get the System and Network Administrators involved
- Alert the line managers
- Coordinate testing with other network activities



Conducting the Test

- Preparations
- Test Monitoring
- Validating and Analyzing the Results

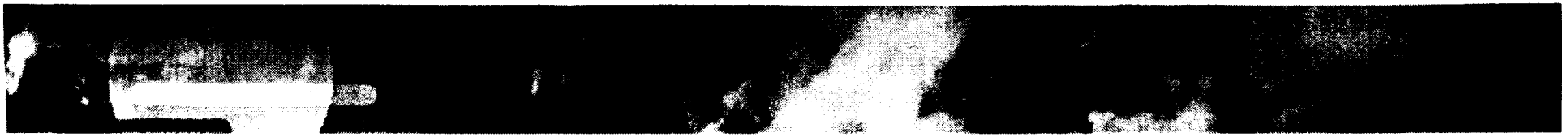
InfoSec World Conference &Expo/2001

Test Preparations

- Make notifications prior to testing
  - Alert those System and Network Administrators being scanned
  - Provide the Help Desk with systems being scanned
- Conduct a test from the outside
  - Test systems from outside the perimeter / Firewall
  - Provides management with the outsider risk

Test Preparations Cont.

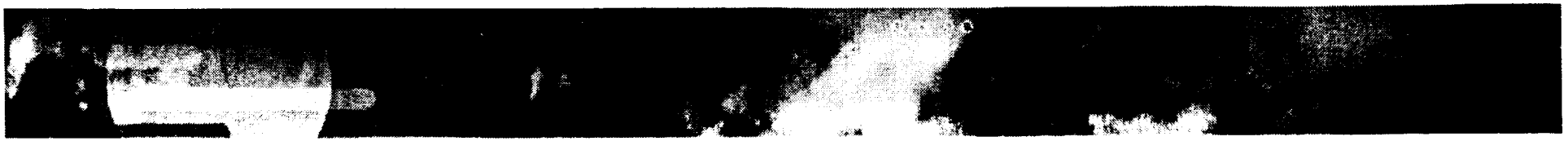
- Conduct tests from behind
  - Test systems behind Firewalls
  - Test systems behind routers and switches that enforce rules
  - Provides management with the insider risk



Test Preparations

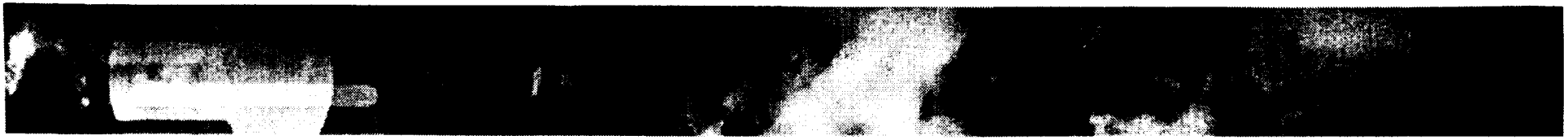
Test Preparations Cont.

- Conduct tests from behind
  - Test systems behind Firewalls
  - Test systems behind routers and switches that enforce rules
  - Provides management with the insider risk



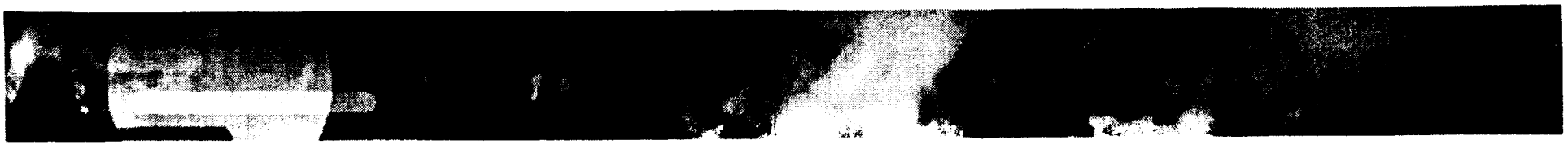
Reporting Test Results

- Establish a Baseline
- Choosing a Report Format
- Presenting the Results to Management



Monitoring the Test

- Are you getting results back?
  - Make sure the software does not hang
  - Check the systems addresses being reported
- Is you test being blocked?
  - Coordinate testing times so that scanning is not blocked
- Did the testing run to completion?
- What percent were actually tested?

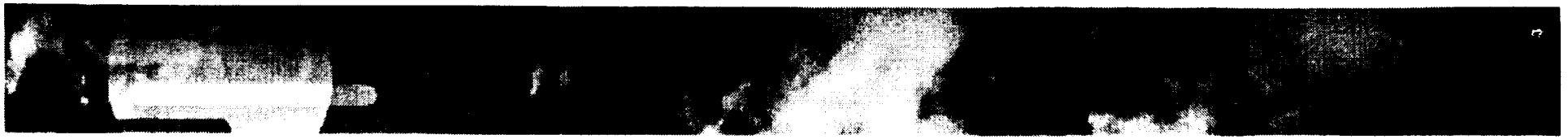


Validate and Analyzing the Results

- Spot check the results
  - Pick some "friendly" System Administrators
  - Ask them to validate the reported vulnerabilities
- Provide results to the responsible System Administrators
- Determine what percent of the system were actually tested

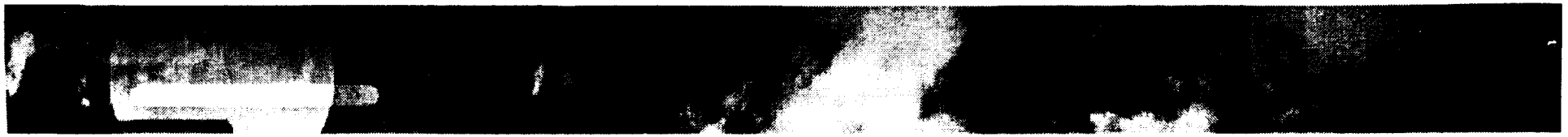
Establish a Baseline

- By the company's security posture (total vulnerabilities)
  - Goal of reducing the total vulnerabilities by a percentage
  - Embarrasses few with little pressure to take corrective action
- By an department/branch security posture (total vulnerabilities)
  - Goal of reducing the total vulnerabilities by a percentage
  - No one wants to be the highest (Red)
  - Embarrasses lots of folks and builds resentments
  - Unfair to those already managing their security risk



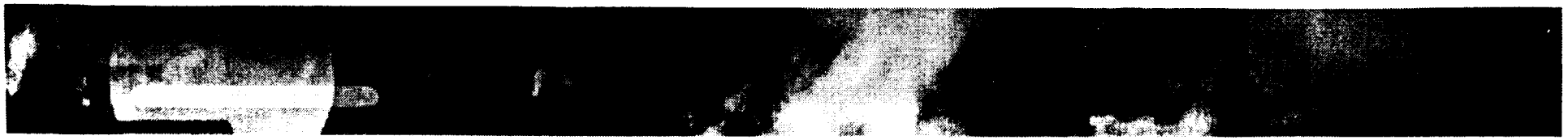
Establish a Baseline Cont.

- By major organization's security posture (total vulnerabilities)
  - Use vulnerabilities as a ratio in each organization
    - Ratio = vulnerabilities detected to systems scanned
  - Goal of reducing the ratio to a target level
  - Enough embarrassment to get corrective actions
  - Number of systems can change will little impact upon the ratio
  - Those practicing good secure are not punished



Choosing a Report Format

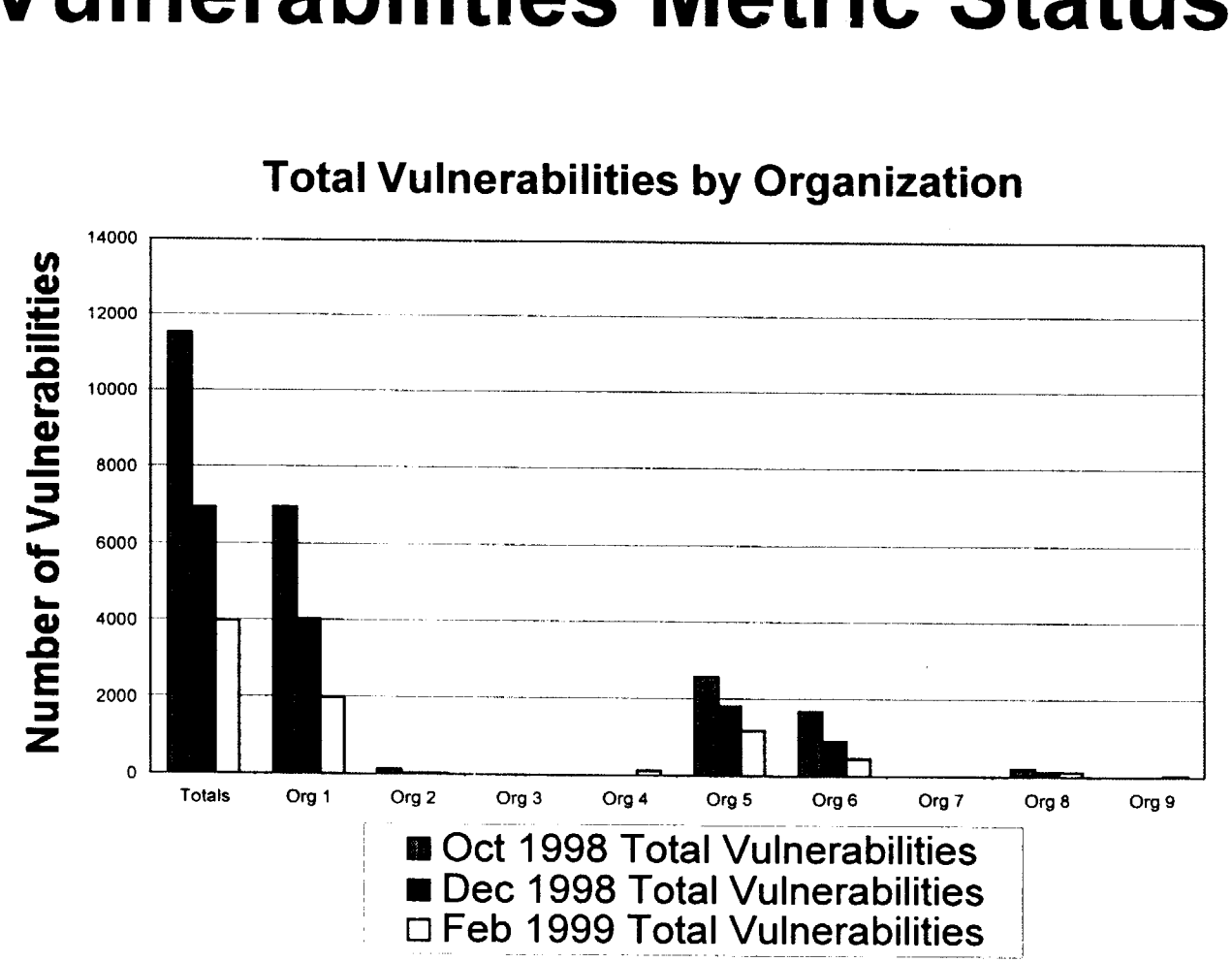
- Numbers, Bars, Pies, or Lines?
- How technical is your target audience?
- How will results from a second or third report look on the chart?



Choosing a Report Format Cont.

- How much time do you have?
  - Have a chart tracking overall company results (improvement over time)
  - Have a chart tracking major organizations' results
    - Show improvements/declines from previous tests
    - Compare all organizations with the target goal

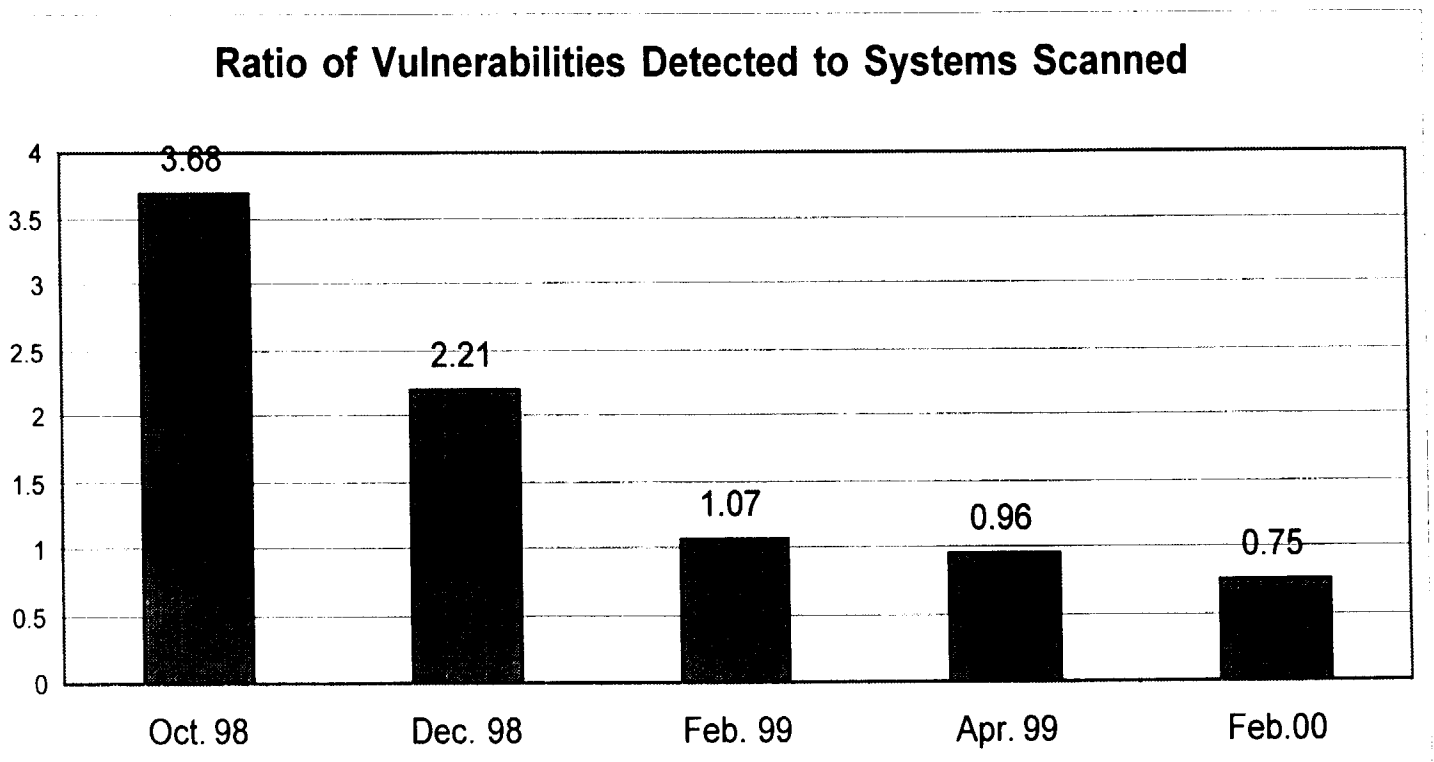
Vulnerabilities Metric Status



InfoSec World Conference Expo/2001

MIS TRAINING INSTITUTE

Vulnerabilities Metric Status

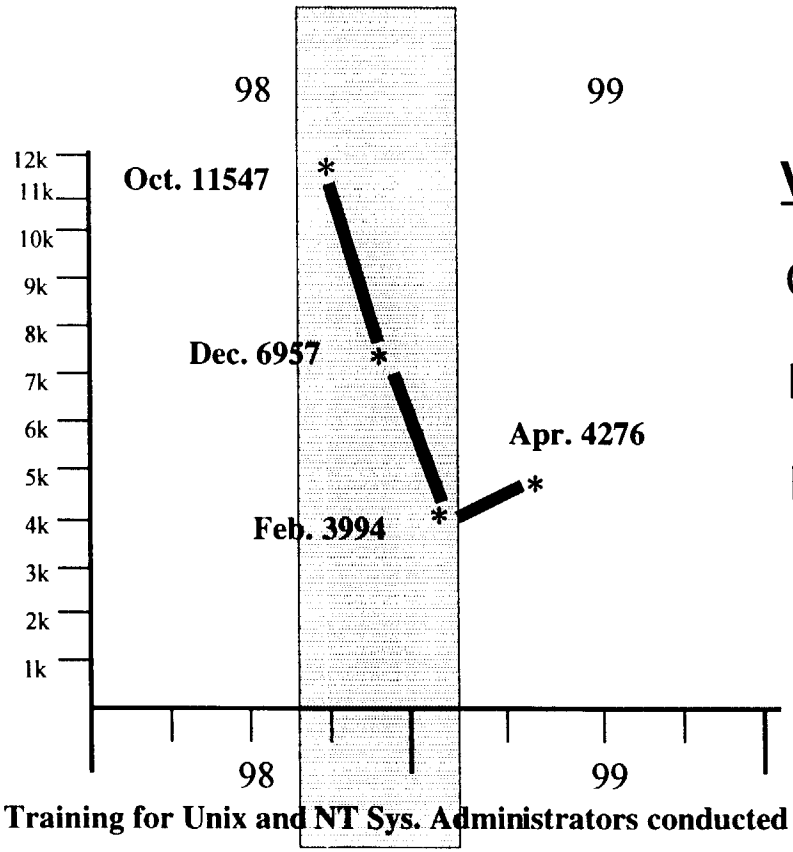


InfoSec World Conference !Expo/2001

MIS TRAINING INSTITUTE

Scanning Program Results

Vulnerabilities Detected by Scans



Ratio
Vulnerabilities / System

Oct. 11547/ 7824 or 1.47

Dec. 6957/ 7903 or .88

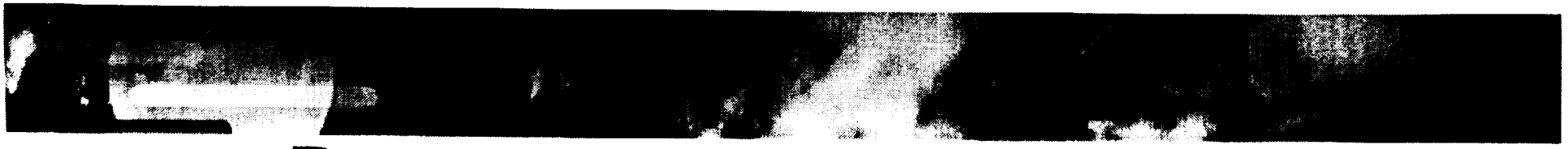
Feb. 3668/ 8566 or .43

Apr. 4276/ 8874 or .48

IT Security Training for Unix and NT Sys. Administrators conducted during this period.

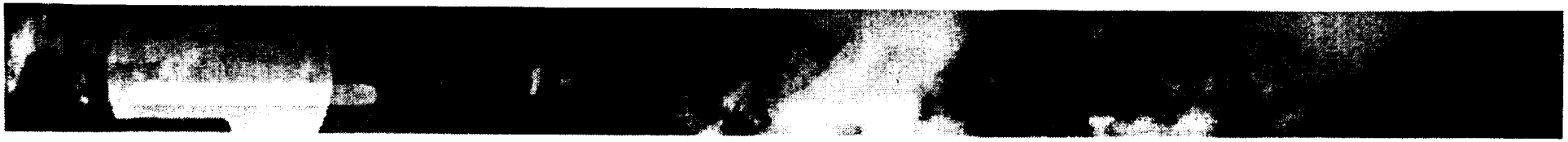
InfoSec World Conference !Expo/2001

MIS TRAINING INSTITUTE



Presenting the Results to Management

- Quick update of the threat/problem
  - News items or "war story"
- Brief reminder of the program goals
- Chart showing latest test results
- Chart comparing current with past results
- Chart showing next scheduled test
- Sit down quickly

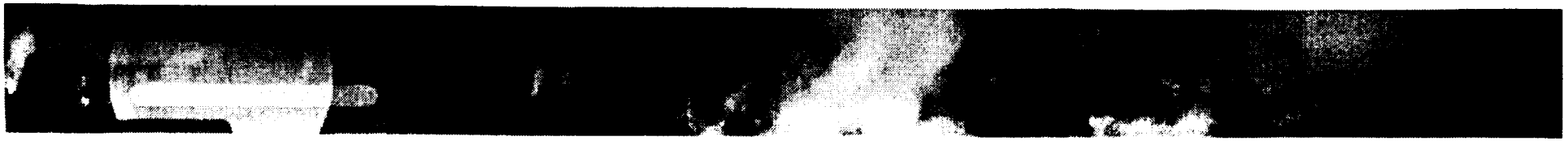


Achieving Compliance

- Work from the Bottom
- Work the Middle Managers
- Play Hardball at the Top

InfoSec World Conference !Expo/2001

MIS TRAINING INSTITUTE

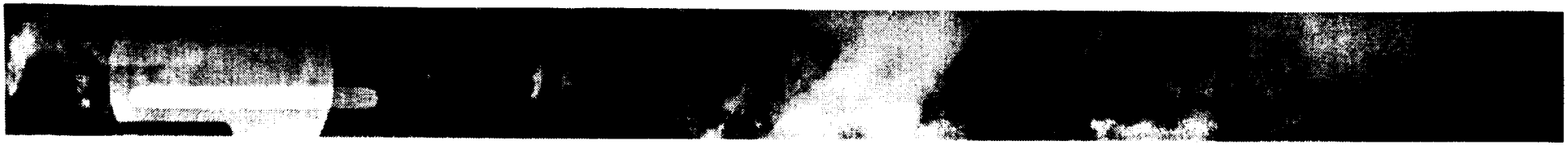


Work from the Bottom

- Encourage System Administrators to test themselves
- Provide the results for review and comment
- Host "Birds-of-a-Feather" meetings for sharing experiences
- Host lunch time seminars on the vulnerabilities and security tools
- Bring in speakers from other companies

InfoSec World Conference Expo/2001

MIS TRAINING INSTITUTE

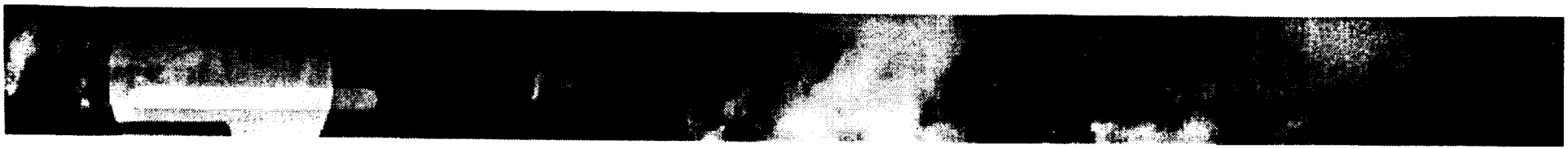


Work the Middle Managers

- Show understanding for their limited resources
  - Offer to give presentations at Staff meeting
  - Keep meeting and briefing short and focused
- Create "Shining Stars"
  - Assist a couple of departments/branches to improve
  - Others will have to show improvements

InfoSec World Conference Expo/2001

MIS Training Institute

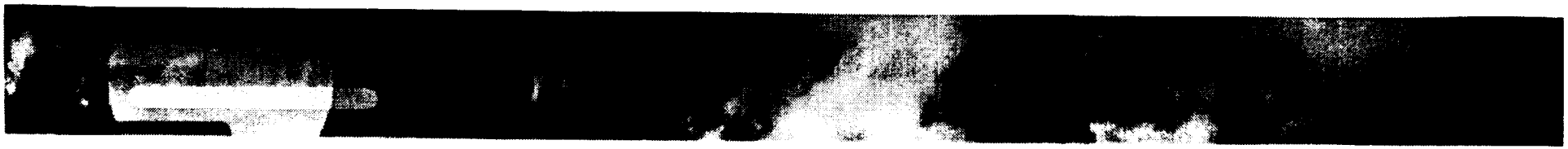


Play Hardball at the Top

- Time with Senior Management is precious
- Regular status briefings are essential
- Milestones must be clear (Stop Light Chart)
  - Zero to 30% improvement: RED
  - 30% to 90% improvement: YELLOW (easy to get yellow)
  - 90% to 100% improvement: GREEN (hard to get green)
- Ensure each organization is on the "Stop Light Chart"
- No one wants to be in last place!

InfoSec World Conference & Expo/2001

MIS TRAINING INSTITUTE

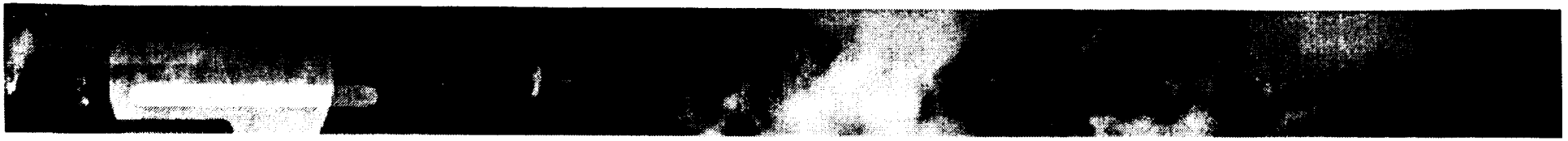


Example "Stop Light Chart"

Company Organizations	Password Problems	Buffer Overflows	Software Outdated	Unused Ports Open	Remote Sharing	Unrestricted Access
Code A		Yellow	Yellow	Yellow		
Code B						
Code C	Green	Green	Yellow			
Code D	Green	Yellow	Yellow			
Code E	Green	Green	Green	Green	Yellow	
Code F	Green	Green	Yellow	Yellow	Yellow	
Code X	Green	Green		Green	Green	Yellow
Code Y	Green	Green	Yellow	Yellow		
Company Total	Yellow	Yellow	Yellow			

InfoSec World Conference & Expo/2001

MIS TRAINING INSTITUTE

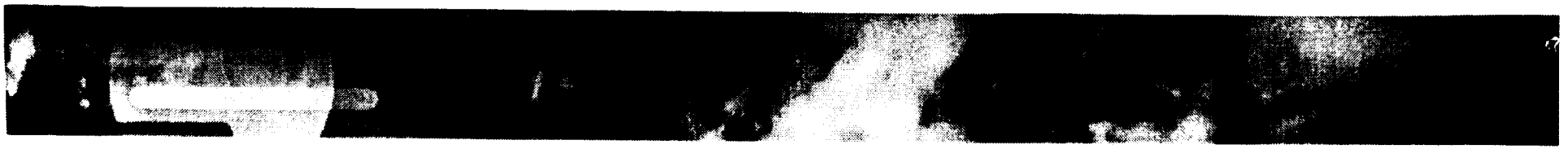


Lessons Learned and Pitfalls

- Vulnerability Testing Tools
- Conducting the Test
- Informing the Community
- Presenting to Management

InfoSec World Conference Expo/2001

MIS TRAINING INSTITUTE



Vulnerability Testing Tools

- Start scanning with a small number and work up to determine your router's load and work closely with your Network Administrator
- Speed up the testing process by targeting a limited number of vulnerabilities
- Ping for valid host - don't test every address you own
- Break up the testing by department/branch - scanning runs better

Conducting the Test

- Give System Administrators advanced warning
  - Prevent logging server denial of service
  - Prepare systems for brute force password testing and failure lock outs
  - Modify router tables to allow (not block) your testing system
- Testing about every 2 months allows time for corrective actions to be taken

Inform the Community

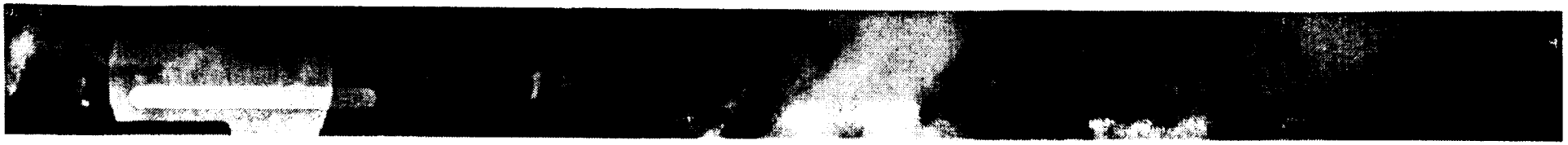
- Avoid working in a vacuum
  - User are afraid that their activities are being monitored
  - System Administrators may feel their skills are being audited

Inform the Community Cont.

- Provide the testing tool; but **BEWARE** not to allow "wayward" testing
  - Ensure you can generate custom keys for System Administrators to use
  - Ask for the addresses they will be testing
  - Be sure they also inform their customers

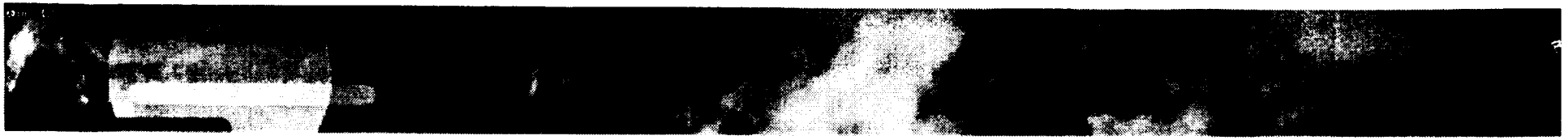
Presenting to Management

- First report to management should be an overview
- First "Stop Light Chart" should have no colors - warning of things to come
- Avoid surprising managers
  - Notify each manager of their result ahead time
  - Provide support for those trying to improve but facing obstacles



A Note About Scan Results

- After the third or forth scan, improvements will begin to level off
  - Fixes cost resources
  - Fixes impact performance
- Solution - Phase II
  - Introduce complex vulnerabilities



Summary

- A good vulnerability testing program can help reduce system compromises
- Provides a way of assessing and measuring improvements in security
- Motivates everyone to get involved